80

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/659,834	09/10/2003	Tamio Saito	7167-102.US/10311148	5947

167 7590 06/21/2005

FULBRIGHT AND JAWORSKI LLP
555 S. FLOWER STREET, 41ST FLOOR
LOS ANGELES, CA 90071

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/659,834	**Applicant(s)** SAITO ET AL.	
	Examiner Brandon S. Hoffman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 April 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-6,9-15 and 17-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-6,9-15 and 17-28* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *4-27-05*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Applicant's arguments, filed April 18, 2005, with respect to claims 3-6, 9-15, and 17-28 have been considered but are moot in view of the new ground(s) of rejection.

Rejections

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 12-14 and 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claims 12-14 and 17 recites the limitation "the security processor" in the third limitation. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

6. Claims 3-6, 9, 10, 18-20, 24, 25, 27, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bromba et al. (U.S. Patent Publication No. 2001/0047479 A1) in view of Shen (E.P. No. 1,074,949).

Regarding claim 3, Bromba et al. teaches comprising:

- **An on-board memory for storing reference data** (fig. 1, ref. num 2)**,**
- **An on-board sensor for capturing live biometric data** (fig. 1, ref. num 1)**,**
- **An on-board microprocessor for comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold** (fig. 1, ref. num 3 and 4)**, and**
- **Means for communicating the verification message to an external network** (fig. 1, connection from 4 to 5 and paragraph 0028)**,**
- **Wherein the verification message includes at least excerpts from the stored reference data** (paragraph 0026), **and**
- Wherein the verification message includes at least excerpts from the captured biometric data (paragraph 0026).

Bromba et al. does not teach the use of an intelligent identification card, but rather an easily accessible device, such as a telephone or computer (paragraph 0022).

Shen teaches the use of an intelligent identification card (fig. 1, ref. num 1).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using an intelligent identification card, as taught by Shen, with the apparatus of Bromba et al. It would have been obvious for such modifications because intelligent identification cards provide a means for a user to carry only one card, which contains cash-like value along with other identification so that the user is not overwhelmed with one card for each transaction.

Regarding claim 4, Bromba et al. as modified by Shen teaches wherein the verification message is transmitted to a remote authentication system for additional verification (see paragraph 0028 of Bromba et al.).

Regarding claim 5, Bromba et al. as modified by Shen teaches wherein the remote authentication system includes remotely stored reference data that is different from the locally stored reference data (see paragraph 0028 of Bromba et al.).

Regarding claim 6, Bromba et al. as modified by Shen teaches wherein the on-board microprocessor uses a different matching algorithm than that used at the remote authentication system (see paragraph 0025 and 0028 of Bromba et al.).

Regarding claim 9, Bromba et al. as modified by Shen teaches wherein the card is ISO Smartcard compatible (see col. 1, lines 6-20 of Shen).

Regarding claim 10, Bromba et al. as modified by Shen teaches further comprising an ISO Smartcard processor (see col. 1, lines 6-20 of Shen, a smartcard that would be used to replace all other cards would inherently be compatible to the ISO standard).

Regarding claim 18, Bromba et al. as modified by Shen teaches wherein the biometric data includes fingerprint data and the sensor is a fingerprint sensor which captures data from a user's finger placed on the sensor (see paragraph 0023 of Bromba et al.).

Regarding claim 19, Bromba et al. as modified by Shen teaches wherein real-time feedback is provided while the user is manipulating his finger over the fingerprint sensor, thereby facilitating an optimal placement of the finger over the sensor (see col. 4, lines 18-23 of Shen).

Regarding claim 20, Bromba et al. as modified by Shen teaches wherein the matching process utilizes a hybrid matching algorithm that takes into account both minutiae and overall spatial relationships in the captured biometric data (see col. 3, lines 42-57 of Shen).

Regarding claim 24, Bromba et al. as modified by Shen teaches wherein the card further comprises means for restricting use of the card to a predetermined location (see col. 1, lines 6-14 of Shen).

Regarding claim 25, Bromba et al. as modified by Shen teaches wherein at least some of the captured biometric data and the reference data are transmitted to a separate authentication server for secure verification of a user's identity priori to any grant of on-line access to an application server for processing of secure financial transactions involving that user (see col. 3, lines 28-36 of Shen and paragraph 0028 of Bromba et al.).

Regarding claim 27, Bromba et al. as modified by Shen teaches wherein the output from the card is used to obtain physical access into a secure area (see col. 1, lines 9-12 of Shen).

Regarding claim 28, Bromba et al. as modified by Shen teaches wherein a record of successful and unsuccessful access attempts is maintained on the card (see col. 4, lines 8-17 of Shen).

Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bromba et al. (US Pub. No. 2001/0047479 A1) in view of Shen (E.P. No. 1,074,949), and further in view of McPhillie et al. (UK Patent Application No. GB 2 2336 005 A)

Regarding claims 11-13, Bromba et al. as modified by Shen teaches all the limitations of claims 3, 9, and 10, above. However, Bromba et al. as modified by Shen does not teach wherein a security processor used for storing and processing the protected biometric data is functionally separated from the ISO Smartcard processor by a firewall, all external data to and from the security processor passes through the ISO Smartcard processor, all external data to and from the ISO Smartcard processor passes through the security processor.

McPhillie et al. teaches wherein a security processor used for storing and processing the protected biometric data is functionally separated from the ISO Smartcard processor by a firewall, all external data to and from the security processor passes through the ISO Smartcard processor, and all external data to and from the ISO Smartcard processor passes through the security processor (fig. 3-5 and page 7, line 7 through page 12, line 21).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine separating the two processors by a firewall and causing all communications in and out of one processor to go through the other processor, as taught by McPhillie et al., with the card of Bromba et al./Shen. It would have been obvious for such modifications because the secure processor can perform the secure calculations, while the unsecure processor can handle regular tasks not dealing with cryptography. This allows more operation-specific processors to be used in the smart card.

Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bromba et al. (U.S. Patent Pub. No. 2001/0047479 A1) in view of Shen (E.P. No. 1,074,949), and further in view of Cassista et al. (U.S. Patent No. 6,385,729).

Regarding claims 14 and 15, Bromba et al. as modified by Shen teaches all the limitations of claims 3, 9, and 10, above. However, Bromba et al. as modified by Shen does not teach the security processor has a first connection used for loading data during a loading process and a second connection connected to an external network and the first connection is permanently disabled after the loading process has been completed.

Cassista et al. teaches the security processor has a first connection used for loading data during a loading process and a second connection connected to an external network and the first connection is permanently disabled after the loading process has been completed (paragraph 0120).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine two connections on the card, one that is disabled after the initial loading is completed, as taught by Cassista et al., with the card of Bromba et al./Shen. It would have been obvious for such modifications because disabling the connection path helps limit the amount of battery draw from the circuit because there is no need to transmit data across that disabled line (paragraph 0120 of Cassista et al.).

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bromba et al. (U.S. Patent Pub. No. 2001/0047479 A1) in view of Shen (E.P. No. 1,074,949), and further in view of Powell (U.S. Patent No. 6,456,980).

Regarding claim 17, Bromba et al. as modified by Shen teaches wherein the biometric sensor is a fingerprint sensor (see col. 3, lines 9-12 of Shen); and the security processor, the ISO Smartcard processor and the fingerprint sensor are all located in a middle region between the upper region and the lower region (see fig. 1 of Shen).

Bromba et al. as modified by Shen does not specifically teach the card comprises an upper magnetic stripe region and a lower embossed region.

Powell teaches the card comprises an upper magnetic stripe region and a lower embossed region (fig. 5A and 5B and col. 4, line 61 through col. 5, line 5).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine an upper magnetic region and a lower embossed region, as taught by Powell, with the card of Bromba et al./Shen. It would have been obvious for such modifications because the upper magnetic region allows for conventional credit card readers to read the card and the lower embossed region allows the users name to be displayed (see col. 5, lines 1-5 of Powell).

Claims 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bromba et al. (U.S. Patent Pub. No. 2001/0047479 A1) in view of Shen (E.P. No. 1,074,949), and further in view of Neuhaus et al. (U.S. Patent No. 6,853,087).

Regarding claims 21-23, Bromba et al. as modified by Shen teaches all the limitations of claims 3 and 18, above. However, Bromba et al. as modified by Shen does not teach wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate, the backing plate comprises a glass epoxy layer sandwiched between two metal layers, and the backing plate is reinforced by a carrier frame surrounding the sheet of silicon.

Neuhaus et al. teaches wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate, the backing plate comprises a glass epoxy layer sandwiched between two metal layers, and the backing plate is reinforced by a carrier frame surrounding the sheet of silicon (col. 4, line 62 through col. 5, line 17).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a silicon fingerprint sensor, epoxy backing, and reinforcing the backing by a carrier frame, as taught by Neuhaus et al., with the card of Bromba et al./Shen. It would have been obvious for such modifications because the materials used provide protection of the chip.

Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bromba et al. (U.S. Patent Pub. No. 2001/0047479 A1) in view of Shen (E.P. No. 1,074,949), and further in view of Krajewski et al. (U.S. Patent No. 5,590,199).

Regarding claim 26, Bromba et al. as modified by Shen teaches all the limitations of claims 3 and 25, above. However, Bromba et al. as modified by Shen does not teach wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid.

Krajewski et al. teaches wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid (col. 6, line 37 through col. 7, line 23).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed which verifies whether the challenge response is valid, as taught by Krajewski et al., with the card of Bromba et al./Shen. It would have been obvious for such modifications because challenge/response systems allow devices to verify a secret without having to exchange the secret in the clear. It would be useful to do this because the devices can ensure security without having to establish a common secret beforehand.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoff

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100